UNIVERSIDADE DE ALFENAS – UNIFENAS

INSTITUTO DE ENGENHARIA E CIÊNCIAS EXATAS – IECEx

DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO – DCC

DISCIPLINA DE INFORMÁTICA GERENCIAL

PROF.: MAURO CESAR BERNARDES

SEGURANÇA COMPUTACIONAL

ALFENAS – MG
MAIO / 1999

Sumário

1 Introdução

Às portas de um novo milênio, é reconhecido que a informação é a fonte vital na busca pelo conhecimento e, por conseguinte, pelo poder. Paralelamente, a obtenção, manutenção e disseminação da informação torna-se uma das maiores preocupações para a sociedade em geral, ocasionando uma crescente expansão das formas de armazenamento e de distribuição através de redes de computadores.

Em contrapartida, tentativas de ataque e invasões consumadas tornam-se freqüentes e envolvem um número crescente de computadores. Desta forma, segurança é a palavra de ordem para a maioria absoluta das empresas em todo o mundo. Com a utilização cada vez maior da tecnologia Internet em ambiente corporativo (as *Intranets*) e sua abertura para o mundo externo (*Extranets*) para atividades essenciais, a preocupação e o risco de invasão dos sistemas empresariais cresceram em um ritmo alucinante nos últimos anos. E não haveria de se esperar algo diferente: os crimes digitais são por vocação muito difíceis de serem descobertos e até mesmo rastreados. Prova disto, é que muitas empresas sofrem invasões em seus sistemas e só se dão conta do fato muito tempo depois, isto quando descobrem.

Mas o panorama esta mudando a passos largos. A cada dia surgem soluções mais robustas de proteção dos dados. *Firewalls*, criptografia de vários bits, certificados digitais, VPNs (*Virtual Private Networks*), *smart cards* e até mesmo biometria (reconhecimento de alguma parte do corpo, como íris dos olhos ou a palma da mão, em substituição às senhas) já fazem parte do arsenal no combate à violação de sistemas e credibilidade das transações on-line.

Como veremos posteriormente nesta mini - dissertação, a tecnologia de segurança de rede mais utilizada hoje em dia é o *firewall*. Este sistema previne a entrada não autorizada utilizando-se de mecanismos de controle de acesso externo. Porém não existe nenhum sistema que possa ser considerado a panacéia em matéria de proteção e ainda, que forneça um elevado grau de segurança enquanto permite uma certa flexibilidade e liberdade no uso dos recursos computacionais.

Existem fatores que tornam muito difícil impedir que atacantes eventualmente tenham acesso a um sistema. A maioria dos computadores possui algum tipo de “furo de segurança” que permite a atacantes externos (ou ainda legítimos) terem acesso a informações confidenciais. Mesmo um sistema supostamente seguro pode ser vulnerável a usuários internos abusando de seus privilégios ou ser comprometido por práticas impróprias. Em vista disto, uma vez que um ataque pode ser considerado inevitável, existe uma óbvia necessidade por mecanismos que possam detectar atacantes tentando penetrar no sistema ou usuários legítimos fazendo mal uso de seus privilégios.

Com o crescente aumento no número de ataques internos, a utilização de mecanismos como o *firewall* deve ser ampliada. Visto que este tipo de ataque, ocasionado pelos próprios usuários do sistema, não permite a localização imediata, torna-se necessário o uso integrado de diversas tecnologias para aumentar a capacidade de defesa de um *site*. Entre estas tecnologias, torna-se interessante a presença de mecanismos que acrescentem características de mobilidade no processo de monitoração do sistema. Desta forma, a introdução de agentes móveis em apoio a segurança computacional apresenta-se como uma solução natural, uma vez que permitirá a distribuição de tarefas de monitoramento do sistema e a agilização no processo de tomada de decisão no caso de ausência do administrador humano.

2 Segurança em Redes de Computadores

2.1 Considerações Iniciais

O termo segurança é usado com o significado de minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos. Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que ele contém [ISO, 1989].

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou de seus dispositivos periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização, formalizada nos termos de uma política de segurança [SOARES, 1995]. Zorkle e Levitt ainda acrescentam que a segurança depende de mais do que a integridade do software e mecanismos de proteção do sistema operacional em uso; ela também é dependente da própria configuração e uso do software [ZERKLE & LEVITT, 1996].

Este capítulo apresenta os principais aspectos de segurança relacionados a redes de computadores, fornecendo um breve resumo das técnicas de detecção de intrusão e abordando alguns sistemas de detecção de intrusão apoiados por diversas técnicas.

2.2 Intrusos e Aspectos de Segurança

Segurança de redes de computadores é uma área de crescente interesse e preocupação, atingindo desde administradores preocupados com a segurança e o bom funcionamento de seus sites até hackers e vândalos buscando novos métodos e técnicas de ataque. O termo hacker deriva da década de 70/80, quando designava pessoas que possuíam um profundo conhecimento sobre computadores, sistemas operacionais e softwares, não tendo nenhuma ligação com os atuais significados no que se refere a atacantes e intrusos. Geralmente os termos hacker e cracker são usados indiscriminadamente, mas algumas diferenciações são encontradas na literatura.

Hacker é o indivíduo com um profundo conhecimento, mas geralmente sem intenções destrutivas. Seu propósito é unicamente provar que consegue invadir um determinado sistema, e quanto mais protegido for este sistema, maior será seu empenho. De forma oposta, o cracker é aquele cujo único objetivo é destruir, danificar e causar perdas. Um estereótipo típico criado é o de um adolescente em sua casa que, a partir de um computador e um modem, profere ataques aos computadores de grandes organizações.

A segurança de uma rede pode ser comparada à segurança de uma casa. Não importa que grau de segurança exista, não importa que sistemas ou trancas sejam usados. Quando alguém decide com suficiente empenho, invadir provavelmente terá êxito. De modo análogo, todas as medidas no sentido de se aumentar a segurança de uma rede tem como objetivo torná-la tão segura quanto possível, já que nenhum sistema conhecido garante o estado - da - arte em termos de proteção. Geralmente, um atacante irá analisar a relação custo/benefício, ou seja, o quão custoso e complicado será invadir um determinado sistema ponderado aos lucros que ele alcançará com tal invasão. Uma vez que esta proporção se torne inviável, pode-se dizer que foi atingido um bom grau de segurança [BONIFÁCIO, 1998].

Ao mesmo tempo em que a Internet é o meio pelo qual a maioria das intrusões e ataques ocorrem, é também através dela que são largamente disponibilizados e veiculados documentos explicando e demonstrando técnicas de hacking, furos de segurança e casos de monitoração de intrusões em andamento. É possível encontrar com facilidade documentos do tipo "receita de bolo", que ensinam passo a passo técnicas de intrusão. Ainda que sejam técnicas simples, podem ser altamente destrutivas, tendo-se em vista que boa parte das redes conectadas à Internet negligencia quase que por completo questões relacionadas à segurança.

Existem atualmente diversos sites dedicados exclusivamente a este assunto, contendo documentos que abordam desde técnicas básicas de hacking até conceitos avançados para se aumentar a segurança de uma rede. Exemplos de site são: http://www.rootshell.com (visitado em 10/12/1998) e http://www.underground.org (visitado em 29/01/1999). Semanalmente são divulgados relatórios com novos furos de segurança nos mais variados sistemas operacionais e softwares. Como existe uma certa demora no lançamento de patches de segurança e uma desconsideração destes patches por muitos administradores de rede, tem-se um cenário em que a maioria das redes se coloca num estado altamente vulnerável.

Esta conjuntura de computadores, redes e comunicações inseguras deve-se, em parte, ao modo como a Internet foi projetada. O principal foco do projeto da Internet, e mais basicamente do protocolo TCP/IP, estava muito distante dos atuais usos da Internet. Seu projeto previa inicialmente o uso por instituições militares e de pesquisa. O crescimento e a popularização da Internet, o surgimento de aplicações de comércio eletrônico, a interligação das redes das diversas filiais de uma empresa e muitas outras características e serviços oferecidos pela Internet de hoje não eram sequer supostas pelos seus projetistas e técnicos. O crescimento da Internet levou a uma mudança no foco e no perfil dos usuários e das aplicações da rede. Em vista disto, os protocolos, serviços, sistemas operacionais como o UNIX e os softwares que são utilizados na Internet não foram projetados e especificados com as devidas preocupações com relação à segurança.

No UNIX, as senhas circulam totalmente abertas pela rede, o protocolo TCP/IP não prevê nenhum esquema de criptografia dos dados ou autenticação das máquinas e usuários envolvidos em uma conexão. Os atuais sistemas, como o Windows NT, foram criados em cenários com preocupações específicas sobre segurança. Porém ainda não se mostraram soluções totalmente confiáveis devido a fatores como pouco tempo para desenvolvimento e testes, o que acarretou em falhas e furos de segurança.

Segurança de redes é um assunto muito vasto e é interessante dividi-lo em duas sub - áreas: Segurança do site e segurança nas comunicações.

2.2.1 Segurança do Site

A segurança do site diz respeito à segurança dos recursos computacionais presentes em uma rede privada. Tais recursos são compostos por hosts, roteadores, impressoras, informações armazenadas, servidores de banco de dados e softwares em geral.

Conforme observado em Reami [REAMI, 1998], quatro princípios básicos definem a segurança de um site:

- **Confidencialidade:** Apenas quem tem os direitos de acessar um determinado recurso ou informação poderá efetivamente acessá-los.
- **Integridade:** Garante que os dados armazenados não serão alterados, tanto como conseqüência de atos provenientes de uma intrusão quanto a eventos como quedas de energia e falhas nos sistemas.
- **Disponibilidade:** Garante que os recursos computacionais e os dados presentes neles estarão disponíveis sempre que necessários. Atualmente um número cada vez maior de ataques exploram furos que causam falhas na disponibilidade dos sistemas. Tais ataques são geralmente chamados de *denial of service*.
- **Autenticação:** Diz respeito à identidade de um usuário, ou seja, garantir se o usuário realmente é quem diz ser.

Uma quebra de segurança pode ocorrer onde existir uma falha. Falhas podem ser atribuídas a três causas principais:

- **Softwares:** Os Softwares que rodam nos computadores podem apresentar falhas que podem ser exploradas por atacantes, ou ainda, falhas que podem prejudicar a rede, como por exemplo, um servidor de banco de dados mal projetado que perca informações. Por outro lado, um software, devido à sua procedência duvidosa, pode conter *backdoors* ou ser um *Trojan Horse* (Cavalo de Tróia).

Um backdoor é um tipo de ataque muito comum em que um software inserido, ou modificado em uma rede pode, a partir de uma combinação especial de caracteres, ou a um evento de tempo, ter um comportamento diferente do esperado. Um dos rastros deixados por uma invasão geralmente são modificações em programas como o deamon de telnet, em que ele é programado para quando alguém entrar com o login hacker, por exemplo, não seja pedida a senha e o acesso seja liberado. Já o Trojan Horse, outro ataque clássico, consiste em se trocar o processo de login por outro programa, de comportamento idêntico. Este programa pede o username e a senha do usuário, salva-o, exibe uma mensagem de erro de senha e chama o verdadeiro processo de login, a partir do qual tudo transcorre normalmente, a não ser pelo fato de que a senha do usuário foi capturada. Para o usuário, tudo ocorre normalmente, ele apenas pensa que digitou errado sua senha.

O outro problema com softwares, como dito anteriormente, é a demora dos fabricantes em lançar patches de segurança de problemas que tenham sido descobertos.

- **Administradores:** A menos que se tenha uma pessoa com a função específica de administrador de segurança, este será outro grande problema. Geralmente, administradores não dão a devida importância à segurança de rede, quer seja por falta de informação ou por desinteresse. As falhas mais comuns oriundas de administradores são: não instalação de sistemas de proteção e auditoria; não aplicação de *patches* de problemas conhecidos; negligenciar procedimentos básicos de segurança; não orientarem os usuários e não se manterem atualizados.
- **Usuários:** Este é outro grande perigo para a segurança de uma rede: usuários mal informados ou mal intencionados podem causar grandes prejuízos. Um ataque se torna muito mais fácil e com muito mais chances de sucesso se proferido por um usuário do próprio sistema com intenções de roubo de informações ou até mesmo vingança contra um colega ou um superior. Usuários comuns podem expor o sistema a senhas fracas, podem fornecer suas senhas para terceiros, utilizar programas de origem duvidosa e muitas outras ações que podem ir contra a política de segurança ou que não estejam previstas, mas que podem colocar a rede sob perigo.

A manutenção de senhas é um fator que esta fortemente relacionada à quebra de segurança. As senhas em sistemas UNIX são guardadas no arquivo /etc/passwd cifradas. Porém o algoritmo usado, chamado de one-way, não permite que a partir da senha cifrada, se obtenha de volta a senha original. Desta forma, o sistema pega a senha do usuário, cifra-a e compara com a que tem guardada. Um intruso, mesmo com acesso ao arquivo de senhas, não tem acesso às senhas originais e, portanto não poderá entrar no sistema. Porém, existe uma técnica chamada de quebra de senha por força bruta na qual o intruso, através de programas chamados de cracker de senhas, escolhe palavras em um dicionário, faz combinações com números, maiúsculas e minúsculas, cifra uma por uma e compara com as senhas cifradas no arquivo de senhas. Quando ele conseguir uma igual, ele terá descoberto uma senha válida para o sistema. Senhas fracas são senhas que podem ser facilmente quebradas, como nomes de pessoas, palavras comuns ou o próprio username. Se todos os usuários possuírem senhas fortes, a chance de que um ataque baseado na captura do arquivo de senhas tenha sucesso seriam pequenas.

Outra grande ameaça são os ataques externos. Ataques externos geralmente se dão de quatro formas diferentes mostradas na Figura 2-1, podendo partir de um único atacante ou um grande grupo. Um ataque pode ocorrer a partir de uma única máquina atacando outra (a), uma máquina sendo atacada por diversas outras (b), várias máquinas sendo atacadas a partir de uma única (c), ou ainda, ser um ataque indireto onde o atacante ataca outra máquina para então realiza o ataque ao seu alvo principal (d).

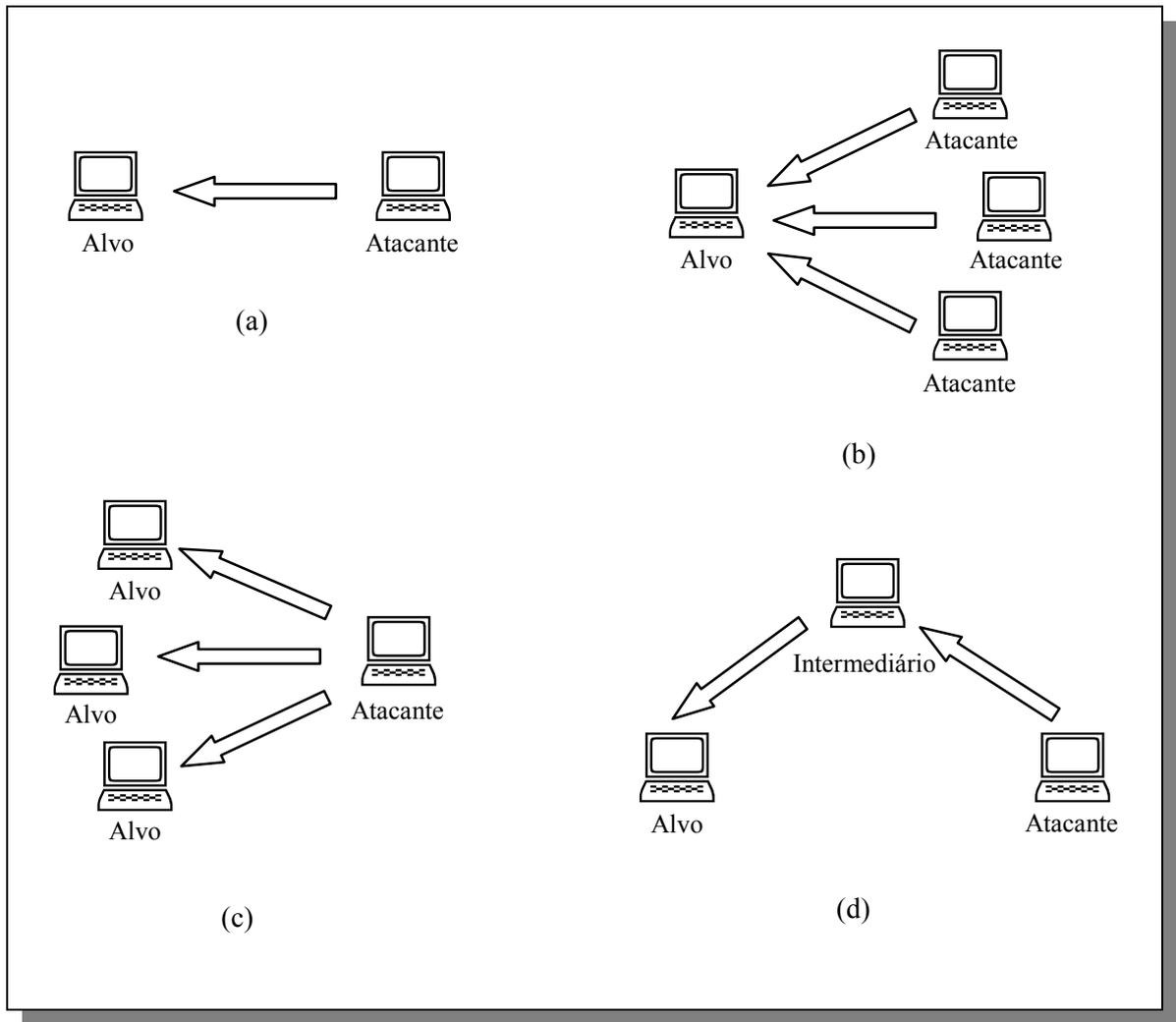
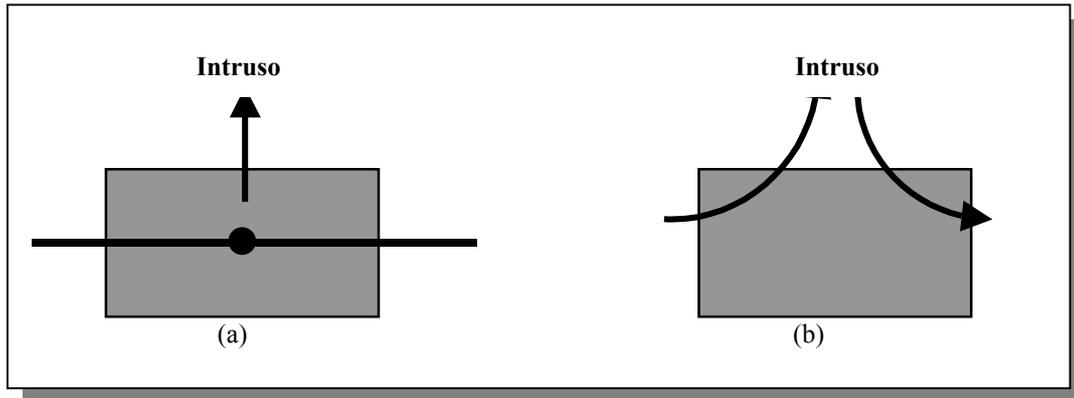



Figura 2-1- Tipos de Ataques Externos

2.2.2 Segurança nas Comunicações

Conceitos de segurança relacionados à comunicações tratam das informações que estão trafegando na rede. Como o protocolo TCP/IP é inerentemente inseguro [BELOVINS, 1989], diversos recursos têm de ser utilizados em conjunto para se aumentar a segurança que o protocolo oferece. As informações que trafegam pela rede através de TCP/IP são abertas, ou seja, qualquer pessoa com acesso ao meio físico pode ter acesso aos dados que estiverem trafegando, bastando para isso, ter uma interface de rede em modo promíscuo, ou seja, todos os pacotes serão capturados, não importando se são destinados a ela ou não. Esta técnica é chamada de sniffing.

Um intruso pode ser classificado em passivo ou ativo. Um intruso passivo simplesmente monitora a rede em busca de informações com senhas, números de cartões de crédito e, informações confidenciais; enquanto que o intruso ativo atua modificando o conteúdo dos pacotes.

Figura 2-2 - Intruso passivo (a) e intruso ativo (b)

Desta forma, é preciso alguns requisitos para se garantir um ambiente em que se tenha segurança nas comunicações:

- **Confidencialidade:** Apenas as partes envolvidas podem ter acesso ao conteúdo dos dados que estão trafegando na rede. Qualquer ação de monitoração da rede não deve ser capaz de ter acesso aos dados.
- **Integridade:** Deve-se garantir que a informação transmitida em um ponto é a mesma recebida em outro e que não houve qualquer adulteração dos dados por partes de terceiros ou falhas.
- **Autenticidade:** As partes envolvidas em uma comunicação devem ter meios de confirmarem mutuamente suas identidades, certificando-se de com quem estão se comunicando.

De forma semelhante à segurança do site, não existe nenhum protocolo ou solução completamente segura. Novos protocolos têm sido propostos e utilizados no intuito de se atingir um alto grau de segurança nas comunicações, protocolos como HTTPS e SSL são voltados a aplicações WEB, enquanto que o protocolo SET (Secure Eletronic Transaction) [SET, 1999] recentemente desenvolvido por grandes empresas como IBM e outras em parceria com a VISA, visam atacar o problema do comércio eletrônico em que existem três partes envolvidas na negociação: o cliente, o vendedor e o banco onde será efetuado o pagamento.

2.2.3 Criptografia

A principal técnica de segurança utilizada para garantir segurança nas comunicações é a criptografia [TANEMBAUM, 1997]. A criptografia surgiu da necessidade de se enviar informações sensíveis através de meios de comunicação não confiáveis, ou seja, em meios onde não é possível garantir que um intruso não irá interceptar o fluxo de dados para leitura ou para modificá-lo. Criptografia consiste em técnicas que permitem transformar um texto legível em outro segundo um algoritmo, de forma que a obtenção do texto original a partir do cifrado seja possível apenas usando-se o mesmo algoritmo. Criptografia teve seu grande desenvolvimento durante a segunda guerra mundial e a guerra fria para garantir que o inimigo não tivesse acesso às comunicações.

A técnica mais simples é a transposição de letras, por exemplo, trocando-se cada letra por sua subsequente no alfabeto: USP → VTQ. Claro que a criptografia usada nos modernos sistemas utilizam algoritmos muito mais complexos baseados em chaves. Após o texto ser cifrado (plaintext) é gerado um ciphertext usando-se como parâmetros uma chave como na Figura 2-3.

Existem dois tipos: criptografia com chave simétrica e criptografia com chaves públicas. Como a recuperação da informação original está vinculada ao conhecimento da chave, um processo para se conseguir quebrar o texto cifrado é o mesmo usado com senhas: busca exaustiva. Neste caso, são geradas todas as possíveis combinações de chaves até que se ache a correta. O grande problema desta solução é que o número de chaves possíveis cresce exponencialmente com o tamanho da chave, e as chaves usadas em aplicações militares

ou de alta segurança podem levar alguns milhares de anos para serem quebradas com os recursos computacionais disponíveis atualmente.

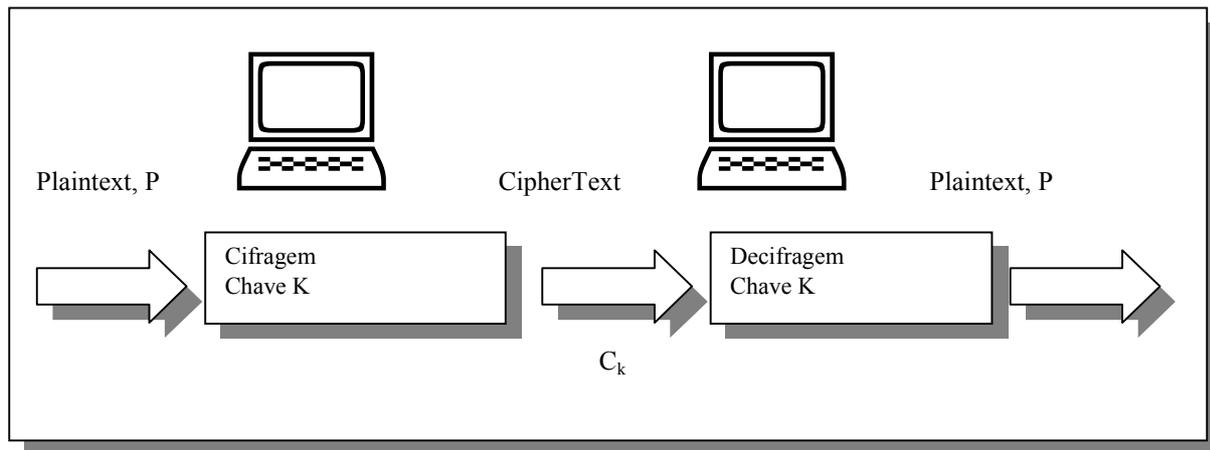



Figura 2-3 - Criptografia Baseada em Chaves

Na criptografia com chaves simétricas, é usada a mesma chave para se cifrar e decifrar um texto. Neste caso, ambas as partes envolvidas tem de concordar com uma chave antes de iniciar a comunicação, o que pode ser problemático, pois a menos que se conheçam, a escolha da chave deve ser feita usando-se a própria rede insegura. Exemplos de algoritmos de chave simétrica são DES (Data Encryption Standard), largamente utilizado no passado pelo governo americano, TrippleDES e IDEA (International Data Encryption Algorihm) [TANEMBAUM, 1997].

A criptografia de chave pública utiliza duas chaves diferentes e complementares. O que é cifrado com uma chave só pode ser decifrado com a outra e vice-versa. O usuário deixa uma chave de conhecimento público (chave pública) e mantém a outra em segredo (chave privada). Este modelo evita as duas partes terem de concordar com uma única chave, uma vez que cada uma conhece a chave pública da outra, podendo com ela, cifrar os textos que só poderão ser lidos pela chave privada correspondente. Algoritmos de chave pública são o RSA (Rivest, Shamir e Adleman, as iniciais dos inventores) e El Gamal, por exemplo.

Com o uso de criptografia, seja por chave simétrica ou pública, pode-se garantir a confidencialidade dos dados que serão enviados em uma conexão. Apesar da criptografia de chave pública ser mais segura que a de chave simétrica, ela é muito lenta para grandes volumes de dados. Atualmente, soluções como o protocolo SSL (Security Socket Layer) da Netscape Comunications [SSL, 1996] utiliza as duas técnicas em conjunto para se assegurar a velocidade. O primeiro passo é usar criptografia de chave pública para que as duas partes possam concordar em uma chave que posteriormente será usada na criptografia de chave simétrica durante todo o restante da comunicação.

O uso de criptografia garante apenas a confidencialidade dos dados, uma vez que um simples ataque do tipo man-in-the-middle, onde uma terceira pessoa está posicionada entre as duas partes que querem se comunicar faz com que cada uma delas acredite estar falando com a outra, sendo que estão ambas se comunicando com esta terceira pessoa. Ou seja, não há meios de se garantir que uma determinada chave pública pertença realmente a alguém. Para isso, existem os certificados digitais. Através desta assinatura, um usuário pode confirmar se uma determinada

chave pública pertence realmente ao seu dono. Certificados digitais estão sendo largamente usados nos browsers Web (Netscape e Explorer principalmente) e se baseiam no conceito de entidades certificadoras que emitem os certificados baseados em suas chaves pública e privada. Como os browsers já tem a chave pública de um certificador, e no qual ele confia, ele pode verificar a autenticidade do portador de um certificado gerado pelo certificador, garantindo-se a autenticidade. Em um certificado digital do tipo X.509 utilizado pelo SSL, vão informações como o nome do dono, data de criação, data de validade, versão e a chave pública do dono cifrada através da chave privada do certificador. Desta forma, garante-se que apenas a chave pública do certificador possa decifrar a chave pública e esta não precisa ser transferida pela rede sem garantias.

2.3 Ameaças e Ataques

Uma ameaça consiste em uma possível violação da segurança de um sistema. Algumas das principais ameaças às redes de computadores são:

- Destruição de informação ou de outros recursos;
- Modificação ou deturpação da informação;
- Roubo, remoção ou perda de informação ou de outros recursos;
- Revelação de informação;
- Interrupção de serviços.

As ameaças podem ser classificadas como acidentais ou intencionais, podendo ambas serem ativas ou passivas. Ameaças intencionais são as que não estão associadas à intenção premeditada (descuidos operacionais, bugs de software ou hardware). A concretização das ameaças intencionais varia desde a observação de dados com ferramentas simples de monitoramento de redes, a ataques sofisticados baseados no conhecimento do funcionamento do sistema. A realização de uma ameaça intencional configura um ataque.

Ameaças passivas são as que, quando realizadas, não resultam em qualquer modificação nas informações contidas em um sistema, em sua operação ou em seu estado. Uma realização de uma ameaça ativa a um sistema envolve a alteração da informação contida no sistema, ou modificações em seu estado ou operação.

Alguns dos principais ataques que podem ocorrer em um ambiente de processamento e comunicações de dados são os seguintes:

- **Personificação**: uma entidade faz-se passar por outra a fim de obter privilégios extras;
- **Replay**: uma mensagem, ou parte dela, é interceptada e posteriormente transmitida para produzir um efeito não autorizado;
- **Modificação**: o conteúdo de uma mensagem é alterado, implicando em efeitos não autorizados sem que o sistema consiga detectar a alteração;
- **Recusa** ou **Impedimento do Serviço**: ocorre quando uma entidade não executa sua função apropriadamente ou atua de forma a impedir que outras entidades executem suas funções;
- **Ataques internos**: ocorrem quando usuários legítimos comportam-se de modo não autorizado ou não esperado;
- **Ataques externos**: ocorrem quando usuários externos ou pessoas não autorizadas conseguem uma conexão externa e realizam ações inesperadas.
- **Armadilhas**: ocorre quando uma entidade do sistema é modificada para produzir efeitos não autorizados em resposta a um comando ou a um evento, ou seqüência de eventos predeterminados.
- **Cavalos de Tróia**: nesse ataque, uma entidade executa funções não autorizadas, em adição às que está autorizada a executar.

2.4 Firewalls

Um mecanismo muito utilizado na prática para aumentar a segurança das redes de computadores, protegendo-as de ataques externos, é o firewall. Um firewall fundamenta-se no fato de que normalmente a segurança é inversamente proporcional a complexidade. Assim, proteger máquinas de uso geral onde são executados diferentes aplicações, de variados portes, é uma tarefa complicada, pois é muito improvável que nenhuma das várias aplicações apresente falhas que possam ser exploradas para violar a segurança do sistema. Desta forma, fica muito mais fácil garantir a segurança isolando as máquinas de uso geral de acessos externos, usando uma barreira de proteção que impeça a exploração das possíveis falhas.

Na configuração de um firewall, as principais decisões relacionadas à segurança são freqüentemente ditadas pela política de segurança da organização ou corporação. Especificamente, as decisões devem ser tomadas pensando-se até que nível a segurança deve ser mais importante que a flexibilidade e facilidade de uso dos recursos computacionais que o firewall se destina a proteger. O princípio da simplicidade tem como conseqüência a seguinte consideração: para diminuir os riscos, a configuração dos firewalls deve ser minimizada, excluindo tudo que não seja estritamente necessário.

Há duas abordagens básicas na configuração de um *firewall*:

- *O que não é expressamente proibido é permitido*
- *O que não é expressamente permitido é proibido*

No primeiro caso, o administrador do sistema tem de prever que tipos de ações os usuários, ou pessoas externas, podem fazer que infringem a política de segurança e preparar defesas contra elas. No segundo caso, o firewall deve ser projetado para bloquear tudo, os serviços devem ser permitidos caso a caso após um cuidadoso estudo de necessidade e risco. Isto causa impacto imediato nos usuários, que podem ver o firewall como um incomodo. Esta opção é também a mais segura, já que o administrador não precisa conhecer profundamente que portas TCP são seguras ou que furos de segurança podem existir no kernel do sistema ou nas aplicações. Uma vez que muitos fabricantes demoram em publicar furos de segurança, esta é claramente uma abordagem mais conservadora, com base no fato de que o que você não conhece pode ser perigoso para você. Esta segunda abordagem pode ser bem empregada em empresas com normas bem definidas e rígidas, porém pode-se tornar altamente imprópria em instituições de ensino e pesquisa, uma vez que ela restringe em demasia o uso dos recursos computacionais. A não ser que se tenha uma equipe muito bem preparada e que reconheça a fundo todas as diferentes necessidades dos usuários do sistema e reflitam isto na configuração, o firewall pode ser tornar um inconveniente e mesmo prejudicar o andamento de pesquisas.

Um firewall, em geral, consiste nos componentes mostrados na Figura 2-4. Os filtros (screens) bloqueiam a transmissão de certas classes de tráfego. O componente gateway é uma máquina, ou um conjunto de máquinas conectadas por um segmento de rede, que fornecem serviços de retransmissão. O filtro colocado na saída (entre a rede externa e o gateway) é usado para proteger o gateway de ataques externos, enquanto o filtro interno protege a rede interna das conseqüências de um ataque que tenha conseguido comprometer o funcionamento do gateway. Assim, os dois filtros atuando isoladamente, ou em conjunto, protegem a rede interna de ataques externos. Um gateway do firewall que pode ser acessado a partir da rede externa é chamado de bastion host. Cabe reafirmar que, fisicamente, os filtros e o gateway podem ser implementados em uma única máquina, ou em um conjunto de máquinas ligadas por um segmento de rede [SOARES, 1995].

Outras formas de configuração são apresentadas na literatura pesquisada. Cada uma apresenta seu ponto forte e também sua fragilidade. Informações mais detalhadas podem ser encontradas em [CHAPMAN, 1992][WACK & CARNAHAN, 1994][BELLOVIN & CHESWICK, 1994].

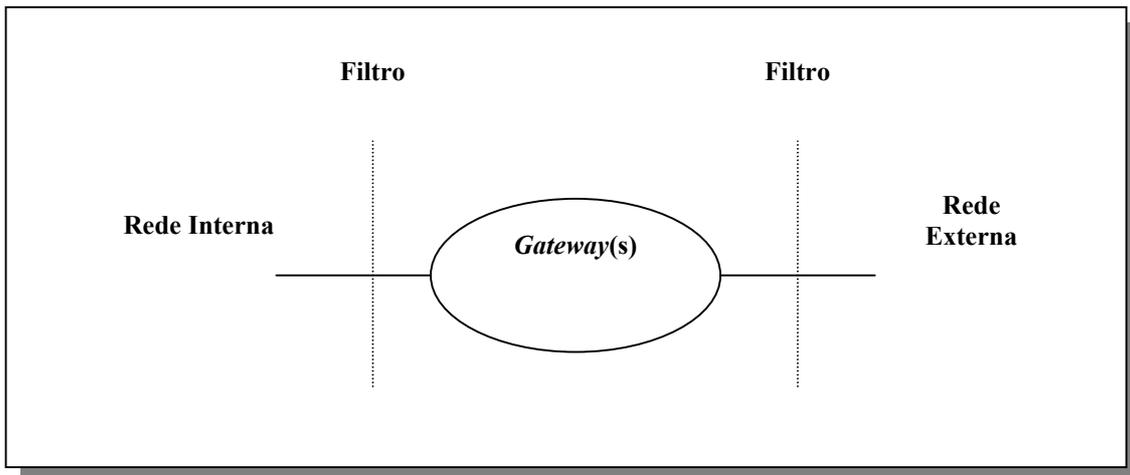



Figura 2-4 - Componentes de um Firewall [SOARES, 1995]

2.5 Política de Segurança

Uma política de segurança é um conjunto de leis, regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos [SOARES, 1995].

Um dado sistema é considerado seguro em relação a uma política de segurança, caso garanta o cumprimento das leis, regras e práticas definidas nessa política.

Uma política de segurança deve incluir regras detalhadas definindo como as informações e recursos da organização devem ser manipulados ao longo de seu ciclo de vida, ou seja, desde o momento que passam a existir no contexto da organização até quando deixam de existir.

As regras que definem uma política de segurança são funções das designações de sensibilidade, associadas aos recursos e informações (por exemplo: não classificado, confidencial, secreto e ultra-secreto), do grau de autorização das entidades (indivíduos ou processos agindo sob o comando de indivíduos) e das formas de acesso suportadas por um sistema.

A implantação de uma política de segurança baseia-se na aplicação de regras que limitam o acesso de uma entidade às informações e recursos com base na comparação do seu nível de autorização relativo a essa informação ou recurso, na designação da sensibilidade da informação ou recurso e na forma de acesso empregada. Assim, a política de segurança define o que é, e o que não é permitido em termos de segurança, durante a operação de um dado sistema. A base política de segurança é a definição do comportamento autorizado para os indivíduos que interagem com um sistema [SOARES, 1995].

Uma quebra de segurança pode ser definida como uma ação, ou conjunto de ações, que vão contra política de segurança vigente. Esta política de segurança é criada com as necessidades particulares de cada local. Desta forma, o que é considerado uma quebra de segurança pode variar conforme o local. A política de segurança irá definir o que pode ou não pode ser feito, por quem, sob quais circunstâncias, define os procedimentos (Plano de Emergência) a serem tomados frente a uma invasão, quais são os recursos que devem ser prioritariamente protegidos, que nível de risco é aceitável, além de resolver questões éticas e polêmicas como, por exemplo, se o administrador ou chefe tem o direito de ler o e-mail dos funcionários. Uma vez que se tenha tudo definido e que cada usuário e administrador esteja ciente desta política, tem-se um quadro onde é fácil identificar que ações são consideradas como uma quebra de segurança e que medidas podem ser tomadas.

2.6 Sistemas de Detecção de Intrusão

Uma intrusão pode ser definida como: "um conjunto de ações que tentam comprometer a integridade, confidencialidade ou disponibilidade de recursos" [CROSBIE & SPAFFORD, 1995].

Apesar do uso dos diversos esquemas de segurança existentes, ainda existe a possibilidade de ocorrência de falhas nestes esquemas e, portanto, é desejável a existência de sistemas capazes de realizar a detecção de tais falhas e informar o administrador da rede. Tais sistemas são conhecidos como sistemas de detecção de intrusão (SDI).

Intrusões são difíceis de detectar porque existem muitas formas pela qual elas podem acontecer. Intrusos podem explorar as fraquezas conhecidas da arquitetura dos sistemas ou explorar o conhecimentos de um sistema operacional para conseguir a autenticação normal de um processo. A tentativa de retirar uma falha do sistema pode introduzir uma nova falha ou expor uma falha existente, dando a oportunidade para um novo ataque.

Tentativas de ataque acontecem de acordo com algumas técnicas de acesso e freqüentemente o invasor está fisicamente fora do sistema sob ataque. Os primeiros modelos de sistemas de detecção de intrusão projetados para computadores isolados usavam algoritmos básicos que incluem análise de funções multinomiais e aproximação de matrizes covariantes para detectar desvio do comportamento normal, bem como sistemas especialistas para detectar violação de políticas de segurança. Os modelos mais recentes monitoram um grande número de redes de computadores e transferem a informação monitorada para ser processada em um equipamento central que emprega técnicas de sistemas distribuídos.

A maioria dos SDIs tem um processo auditor (daemon) em cada máquina, responsável por capturar ações de violação de segurança dentro da máquina. Sistemas baseados em redes, ao invés de utilizar pistas de auditoria, analisam o tráfego de pacotes dentro da rede para detectar comportamento intrusivo.

As funcionalidades de um sistema de detecção tornam-se de vital importância na medida em que fornecem meios de inferir sobre o conteúdo das conexões permitidas e detectar as que apresentem um comportamento suspeito ou não condizente com a política de segurança implantada.

2.6.1 Classificação dos Sistemas de Detecção de Intrusão

Os SDI são classificados sob diferentes ópticas na literatura da área. As principais classificações utilizadas são em termos da forma como o sistema aborda o problema de detectar intrusão e em termos do tratamento dos dados.

As três principais abordagens para detecção de intrusão são: detecção de anomalias, detecção de uso indevido e detecção híbrida.

Sistemas de detecção de anomalias definem um modelo de atividade normal através de perfis de atividade dos usuários e qualquer desvio significante da norma estabelecida é considerado anômalo. Por sua vez, sistemas de detecção de uso indevido definem especificamente que ações do usuário podem constituir um uso indevido do sistema e usam regras definidas, a priori, para codificar e detectar padrões de intrusão conhecidos. Cada uma das abordagens é mais adequada para certos tipos de ataque e, por isso, muitos sistemas utilizam uma abordagem híbrida para tornar a detecção mais eficiente.

Em termos do tratamento dos dados, existem sistemas baseados em rede e sistemas baseados em host. Sistemas baseados em rede examinam os dados que trafegam pela rede através da monitoração on-line dos pacotes. Por outro lado, sistemas baseados em host analisam dados de auditoria recolhidos normalmente pelos sistemas operacionais e buscam de diversas formas pelos padrões de ataque.

As próximas seções apresentam apenas alguns dos muitos SDIs existentes e que utilizam diversas abordagens para resolver o problema de detecção.

2.6.2 Sistemas Especialistas Baseados em Regras

Sistemas especialistas baseados em regras são sistemas inteligentes que capturam conhecimento de especialistas humanos em domínios limitados do conhecimento, geralmente, na forma de regras do tipo IF-THEN. Alguns trabalhos vêm sendo realizados para utilizar esta técnica de inteligência artificial em sistemas de detecção de intrusão.

O SRI International desenvolveu um dos primeiros sistemas baseados nesta técnica o IDES (Intrusion Detection Expert System) apresentado em [LUNT & JAGANNATHAN, 1988]. A evolução deste sistema foi o NIDES (Next Generation Intrusion Detection Expert System) [JAVITZ et al., 1993].

Atualmente, o SRI está desenvolvendo o EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) como sucessor do NIDES. O EMERALD representa uma evolução das pesquisas anteriores com o intuito de acomodar a monitoração de grandes redes e sistemas distribuídos. Este sistema apresenta uma arquitetura altamente modular e permite a integração de novas características facilmente, inclusive a integração de sistemas fornecidos por terceiros [PORRAS & NEUMANN, 1997].

2.6.3 Sistemas Baseados em Data Mining

Lee e Stolfo [LEE & STOLFO, 1997] apresentam uma abordagem baseada em técnicas de data mining para descobrir padrões úteis e consistentes das características do sistema que descrevem os comportamentos de usuários e programas. A partir daí, o conjunto de características relevantes do sistema é usado para computar classificadores (aprendidos por indução) que podem reconhecer anomalias e intrusões.

No trabalho referenciado, Lee e Stolfo afirmam que o maior desafio para a utilização de técnicas de data mining na detecção de intrusão é a imensa quantidade de dados de auditoria necessários para computar os conjuntos de perfis de uso do sistema. Como o processo de aprendizado (mining) é caro em termos de tempo e de armazenamento; e como o processo de detecção em tempo real precisa ser leve e rápido para ser praticamente utilizável, seria impossível de se ter um sistema de detecção de intrusão monolítico. Assim, eles propõem uma arquitetura na qual existem dois tipos de agentes inteligentes: agentes de aprendizado e agentes de detecção. A Figura 2-5 apresenta a arquitetura sugerida por Lee e Stolfo.

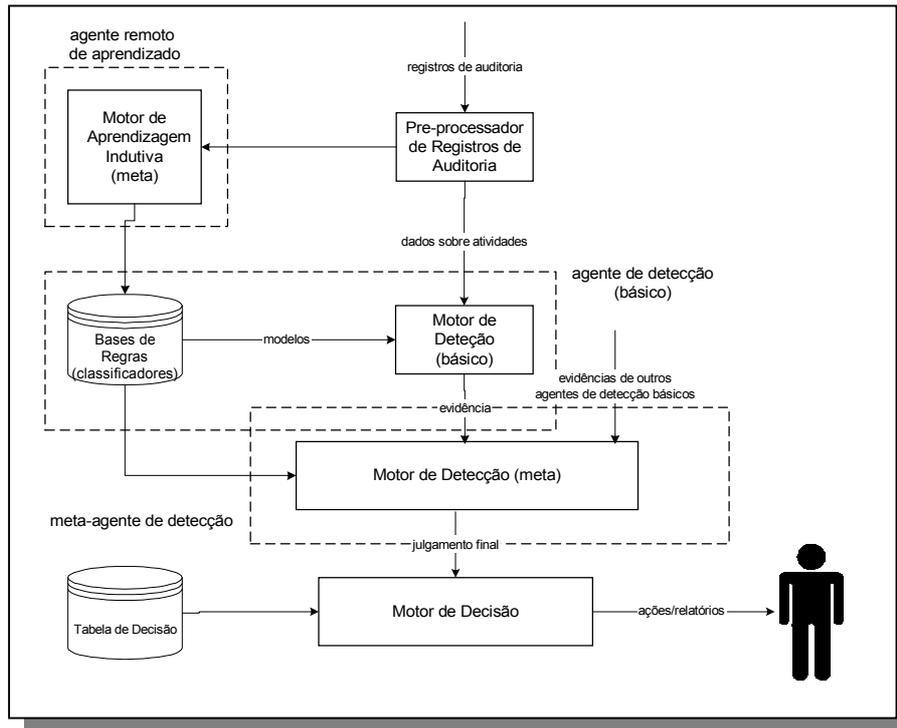



figura 2-5 - Arquitetura de um Sistema de Detecção de Intrusão Baseado em *Data Mining*

2.6.4 Sistemas Baseados em Agentes Autônomos

As utilizações de agentes autônomos têm sido propostas por alguns autores como forma de construir sistemas de detecção de intrusão não - monolíticos. A capacidade dos agentes autônomos de manter informação específica do seu domínio de aplicação, nesse caso, aplicação de segurança, dá a estes agentes grandes flexibilidades.

Crosbie e Spafford especificam um sistema deste tipo no qual as capacidades dos agentes são modificadas através do uso algoritmos genéticos. Os autores reconhecem, entre outras, as seguintes vantagens de sistemas baseados em agentes autônomos sobre sistemas monolíticos [CROSBIE & SPAFFORD, 1995a; 1995b]:

- **fácil configuração:** uma vez que é possível ter uma série de pequenos agentes especializados em tarefas específicas de detecção, o sistema de detecção pode ser configurado da forma mais adequada para cada caso; a adição e remoção de agentes do sistema é facilitada;
- **eficiência:** agentes podem ser treinados previamente e otimizados para que realizem suas tarefas da maneira a gerar a menor sobrecarga do sistema possível;
- **capacidade de extensão:** um sistema de agentes pode ser facilmente modificado para operar em rede e permitir migração para rastrear comportamentos anômalos através da rede, ou mover para máquinas onde eles podem ser mais úteis;
- **escalabilidade:** para atuar em sistemas maiores, basta adicionar mais agentes e aumentar sua diversidade.

Recentemente, o COAST (Computer Operations, Audit and Security Technology, Computer Science Departament at Purdue University) liberou uma implementação de um ambiente que segue as idéias do sistema proposto por Crosbie e Spafford. Este ambiente denominado Autonomous Agents for Intrusion Detection (AAFID) foi implementado utilizando-se a linguagem de scripts Perl e diversos recursos de administração de sistemas e segurança comuns em ambiente

UNIX. O ambiente AAFID possui duas entidades distintas que suportam a execução dos agentes do sistema: Transceivers e Monitors, sendo estes últimos entidades de mais alto nível, que podem detectar possíveis eventos intrusivos não notados por entidades mais simples como Transceivers. As informações preliminares sobre o sistema AAFID podem ser encontradas em Zamboni [ZAMBONI et al, 1998].

Outro trabalho recente na área de aplicação de agentes autônomos em sistemas de detecção de intrusão é apresentado por Barrus e Rowe [BARRUS & ROWE, 1998]. A idéia dos autores é utilizar agentes autônomos estáticos que se comunicam através de um sistema de mensagens de alerta através de uma arquitetura distribuída. Algumas abordagens interessantes sugeridas são: a utilização de agentes especializados na detecção baseada em anomalia e na detecção baseada em uso indevido; e a criação de objetos específicos para tratar os diversos tipos de ataque.

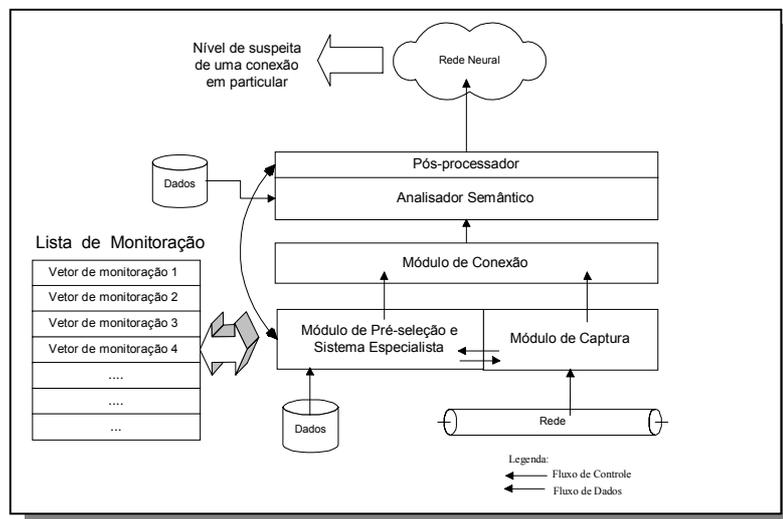
Em sua tese de mestrado, Reami [REAMI, 1998] apresenta a especificação e prototipagem de um ambiente de gerenciamento de segurança computacional apoiado por agentes móveis. O ambiente especificado e prototipado pode ser considerado um avanço importante, pois, além de fornecer recursos tecnológicos avançados e consoantes com o desenvolvimento da área, permite uma abordagem holística do problema do gerenciamento de segurança.

2.6.5 O Sistema de Detecção de Intrusão do ICMC

Uma das características inovadoras deste sistema de detecção de intrusão consiste em introduzir um agente de segurança capaz de detectar comportamento intrusivo em conexões estabelecidas [CANSIAN et al., 1997a, 1997b, 1997c] [BONIFÁCIO Jr. et al., 1998a]. Este agente atua capturando e decifrando pacotes que são transmitidos através da rede sob monitoramento. Para fazer uma inferência sobre a condição de segurança das conexões, o agente emprega um sistema especialista e uma rede neural que irá prover um coeficiente de suspeita, o qual, baseado em informações intrusivas previamente registradas, dará uma idéia a respeito da severidade do ataque ou o grau de suspeita das atividades naquela conexão.

O sistema se baseia no fato de que uma intrusão pode ser detectada a partir de uma análise de modelos predeterminados, que são anômalos se comparados com ações normais. A grande maioria dos ataques é resultado de um pequeno número de ataques conhecidos, como relatados por equipes como o CERT.

O uso de redes neurais pode fornecer mecanismos para o reconhecimento de ataques, bem como uma capacidade de adaptação em resposta a mudanças nas técnicas de intrusão. A Figura 2-6 mostra a arquitetura global do sistema.

Figura 2-6 - Arquitetura global do sistema de detecção de intrusão do ICMC

2.7 Considerações Finais

A literatura tem mostrado que o uso integrado das diversas técnicas apresentadas neste capítulo é, certamente, o melhor método de prevenção e tratamento dos problemas de segurança. Como as tarefas executadas por cada uma das técnicas são muitas vezes complementares e poucas vezes redundantes, a troca de informações entre os sistemas (p.e.,detecção de intrusão e firewall) permite uma atuação mais consistente e eficaz na determinação dos problemas de segurança e na solução dos mesmos, seja ela manual ou automática.

Alguns exemplos de trabalhos nesta linha de pesquisa são apresentados por [BONIFÁCIO Jr. et al., 1998b] e [MOUNJI & LE CHARLIER, 1997]. Outro sinal da tendência de integração dos sistemas de segurança é o estudo de um protocolo para troca de informações entre dispositivos e sistemas relacionados a segurança, denominado IDIP (Intrusion Detection and Isolation Protocol), que está sendo pesquisado e desenvolvido por parceiros como Boeing, Trusted Information Systems e University of California at Davis com financiamento do DARPA [DARPA, 1997].

Como visto, uma recente tecnologia de suporte à segurança em redes de computadores é a introdução do uso de Agentes Autônomos. O conceito de Agente e sua utilização no apoio a segurança são discutidos nos próximos capítulos.